Application No.: 09/767,292 Docket No.: 00-VE04.75B CIP

REMARKS

Independent claims 1 and 25 are amended to emphasize an aspect of the invention so as to more clearly distinguish over the applied art by requiring that the signaling security gateway be responsive to any encrypted time stamp so as to authenticate a control message and, in response, determine if the control data messages are proper including timely and properly sequenced. The amendments are made to more clearly distinguish the invention including the claimed feature over the applied art so as to advance prosecution without disclaimer, waiver or prejudice to include claims of similar to that of the original claims or any other scope supported by the present disclosure in a subsequent continuing application.

This aspect of the invention had been previously emphasized and claimed in, for example, claim 3. The disclosure itself is replete with material describing and emphasizing this aspect of the invention including, for example, the following portions of the specification:

Page 12, lines 19 – 24:

> Message authenticity is verified using digital signatures and **time stamps**. Thus, the Security Gatekeeper functions as a certification agent or authority (CA) for the LEC's SS7 network and interfaces with other and/or higher level CAs to obtain and maintain required digital certificates. **Use of a digital time stamp both ensures non-reuse of signatures and *provides for time-outs so that old or superceded messages are identified and processed appropriately*.**

Note that the highlighted language provides a particularly advantageous feature according to embodiments of the invention in that digital signatures and time stamping prevents copying a previous message and resending it so as to defraud a Local Exchange Carrier (LEC) from realizing the associated revenues.

Further support is found at:

Page 13, lines 11 – 13:

> According to a feature of the invention, the signaling system security monitor functions as a certification agent to exchange and maintain encryption key certificates and may further be configured to **issue and decrypt digital time stamps**

Page 21, lines 5 – 6:

Message authentication is also implemented by the Security Gatekeeper using **time stamped**, digital signatures and/or digital certificates.

Page 25, lines 19 – 21:

The Security Gatekeeper further enhances authentication and verification of ***message sequencing and timeliness*** by appending or encoding messages with digital signatures and **timestamps**.

Page 39, line 13 – Page 40, line 4:

The Security Gatekeeper may also check the digital certificate of the OPC device or system and the **timestamp** of the message to ensure that the message is authentic ***and timely***.

Page 41, lines 20 – 30:

The Security Gatekeeper incorporates data encryption techniques including digital signatures and **time stamps** to maintain system security and enhance message authentication processing. Protocols supporting IP telephony and other IP-based transport of services employ security techniques to assure the source validity of messages. One such technique employed is IP Security Protocol (IPSec). IPSec provides the ability to use encryption technology to certify the authenticity of the source through use of an unalterable, easily verifiable digital signature and **time stamp**. Unfortunately, no equivalent verification tool or instrument is available for basic call setup messages in the SS7 message domain. Instead, the Security Gatekeeper provides a digital signature and **time stamping** capabilities in the SS7 Integrated Services Digital Network User Part (ISUP) protocol messages.

Page 42, lines 1 – 9:

The Security Gatekeeper also performs Originating Point Code digital signature processing and **timestamp** authentication. This processing further enhances network security since, when interconnecting the SS7 Signaling Networks to an IP based, packet or other SS7 networks is desirable to authenticate these interconnecting networks. The Security Gatekeeper supports this authentication function by providing the ability to certify the Originating Point Code (OPC) of outgoing messages and authenticate the OPC of incoming messages with encrypted digital signatures. The digital signature is encrypted based upon Appendix F of T1.655 1996 SS7 Upper Layer Security Capabilities.

Page 42, lines 14 – 16:

> The Gatekeeper thereby functions as a Certifying Agent for all network nodes within its domain, certifying their point codes with an encrypted digital signature of the point code and **timestamp.**

The Examiner had previously responded to aspects of this limitation as presented in claim 3:

> *In reference to claim 3*, wherein the signaling system security monitor is configured to issue and decrypt time stamps.
>
> Bissel do not disclose the use of digital time stamps.
> Sawyer discloses the us of digitally signed time-stamp (column 5 liens 40 -47).
> At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital time-stamps as in the system of Sawyer in the system as disclosed in applicant admitted prior art. One of ordinary skill in the art would have been motivated to do this because it would protect against certificate replay.

While, as asserted by the Examiner, Sawyer does mention use of a time stamp, as further recognized by the Examiner, this is to "thwart a replay of the certificate". Sawyer does not so much as hint at the use of a time stamp to authenticate control date messages and, "in response, determine if said control data messages are proper" including timeliness and proper sequencing of the messages.

Bissell describes no more than conventional encryption mechanisms for authentication. Digital time stamping is a specific piece of data that is encrypted using an encryption technique such as the Triple DES that Bissell alludes to. While Bissell may use this information to defeat certificate replay, there is no suggestion to use a time stamp to authenticate a message so as to determine that it is timely and properly sequenced. It should be recognized that there is a significant difference between encrypting a message and appending an identity key to a message and cryptographically signing the two pieces of information so that the recipient can verify that the message came from the true original source. As Bissell fails to disclose the use of digital signature of time stamps, the subject matter of independent claims 1 and 25 is patentably distinguishable over the combination of references as applied.

Further, as previously urged, it should be noted that there is a significant difference between applicants' invention and the teachings attributable to the Bissell patent. In particular, Bissell describes authentication mechanisms for use between an end terminal, such as a residential computer and a network authentication server as might be used when logging into an ISP. The "OFF HOOK" mentioned throughout the Bissell disclosure and incorporated into the corresponding claims is a protocol message for a telephone set. The relationship described by Bissell is between the access side of a PSTN switch or IP network (i.e., DTE, DCP, CPE) and a server connected to the DTE through the use of the PSTN connection. In contrast, applicants' invention is directed to embodiments that are **internal** to the PSTN network and the signaling that is required to establish the type of connection that Bissell might use to exchange his authentication information. That is, Bissell describes authentication to a database that has a telephony-type communications transport link between the terminal and the database, not to:

> *a signaling system security monitor, separate from the central office switching systems, said signaling system security configured to evaluate an encrypted portion of said control data messages so as to authenticate corresponding ones of said control messages and, in response, determine if said control data messages are proper*

as required by the rejected claims.

Applicants do not contend that security authentication techniques, such as IPSec, Secure Hashing Algorithm (SHA) and other authentication arrangements standing alone were new at the time of the invention. To the contrary, such techniques were already known to those skilled in the art of electronic security. However, what applicants maintain is unique is the application of these security techniques to a particular problem that results in a new and non-obvious solution to a previously, if not unidentified, unsolved problem.

The Examiner's rationale for incorporating the teaching of Bissell is that "[o]ne of ordinary skill in the art would have been motivated to do this because the system would remove the call set-up procedure carried out by the customer, which would remove the inconvenience from the customer." However, it is unclear how such motivation, even if proper, would apply to modification of the admitted prior art described in the instant application to incorporate the teaching of Bissell. Instead, the rationale provided by the Examiner appears to be that provided

by Bissell for implementing an authentication code to be used by a terminal to authenticate itself to the network, i.e., such motivation is the motivation for Bissell but is inapplicable to the subject matter of applicants' invention That is, according to Bissell, requiring a customer to manually provide some form of authentication is "an inconvenience which it would be advantageous to remove from that part of the call set-up procedure carried out by the customer." Bissell at column 1, lines 47 – 49.

In response, the Examiner has taken the position that "[t]he motivation of Bissell is top improve the applicant admitted prior art with the authentication process as disclosed by Bissell. Therefore motivation t create applicants' application would include hindsight. The improvements disclosed by the invention of Bissell would include the improvement that the terminal would have an authentication process that would not inconvenience the user."

If it is the Examiner's position that hindsight reconstruction of the pending claims is proper and may form the basis of the rejection, then clarification is requested as such is clearly contrary to black letter patent law. In any case, the Examiner's line of reasoning supporting the combination is not clear and clarification is requested.

It is again emphasized that the background of applicants' invention involves an interconnection between networks, not access by a customer using a terminal. There is no issue of customer convenience since the customer has no interaction with the signaling network or the control data messages carried by that network. The motivation relied upon by the Examiner as the basis for application of Bissell is simply inapposite to the technological background of the instant invention. The purpose of the various embodiments of the invention is not to facilitate authentication on behalf of benign networks; it is to deny access to unauthorized or spoofed messages by means of authentication.

The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In *re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." (916 F.2d at 682, 16 U.S.P.Q.2d at 1432.). See also In *re*

Fritch, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992) (flexible landscape edging device which is conformable to a ground surface of varying slope not suggested by combination of prior art references).

Even if the asserted combination would result in rendering any of the claims obvious, the lack of motivation therefore makes the combination improper. It is well established that, even if all aspects of the claimed invention were individually known in the art, such is not sufficient to establish a prima facie case of obviousness without some objective reason to combine the teachings of the references. *Ex parte Levengood*, 28 U.S.P.Q.2d 1300 (Bd. Pat. App. & Inter. 1993). It is, therefore, incumbent upon the Examiner to provide some suggestion of the desirability of doing what the inventor has done in the Examiner's formulation, imposition and maintenance of a rejection under 35 U.S.C. § 103(a). "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 U.S.P.Q. 972, 973 (Bd. Pat. App. & Inter. 1985).

Accordingly, for the reasons presented, claims 1 - 24 are considered to be non-obvious over the art of record and withdrawal of the outstanding rejection under 35 U.S.C. 103(a) is respectfully requested.

The claims dependent from claim 1 (i.e., claims 2 – 24) are considered to be allowable both as dependent from the allowable subject matter of claim 1 and further as reciting additional subject matter not found in or rendered obvious by the applied art. For example, claim 7 recites

> *The communications network according to claim 1 wherein said signaling system security monitor includes a memory storing states of respective ones of said central office switching systems, said processor additionally responsive to said states for determining if said control messages are proper.*

Addressing this claim, the Examiner takes the position that:

> *Bissell discloses operation of a telephony service may be modeled in terms of a sequence of states a call may go through. Bissell uses the off-hook condition to define when and how authentication is initiated (column 8 lines 9-50); and therefore when the control messages are proper.*

However, as previously explained, even if Bissell recognizes that there are various states of a system, this does not render obvious the cited claim language which requires not only that a system include states (as broadly do all systems) but that the system states be stored and form a basis to determine if a control message is proper. Thus, even if correct, the mere realization that there are states is insufficient to defeat patentability of the storage and use of this state information to protect a network from improper control messages.

The remaining dependent claims also recite subject matter not described or suggested by the prior art. For example, claim 6 recites:

> The communications network according to claim 1 wherein said signaling system security monitor is configured to selectively enable and inhibit said signaling gateway from exchanging said control data messages between said remote communication network and said signaling communication system in response to said encrypted portions of said control data messages.

This feature prevents the unauthorized use of service. It is to be expected that the applied art would fail to address this problem or provide a solution thereto as it is not directed to providing a secure interface to allow a third party, such as a Competitive Local Exchange Carrier (CLEC) to interface with the network of an incumbent Local Exchange Carrier.

In connection with claims 18 – 24, the Examiner relies on Hanson in formulating the outstanding rejection of those claims. However, as previously explained, Hanson is drawn from non-analogous art. Hanson is directed to a voice mail system providing the creator of a voice mail message with an ability to pre-define a response to the message. This has nothing to do with mediating control messages transmitted between communications networks, the field to which the instant application is directed. This dissimilarity of technological fields is evidenced by the disparity of classifications assigned to the Bissell and Hanson patents. In this case, the

prior art reference is not in the field of applicants' endeavor or reasonably pertinent to the particular problem with which the inventor was concerned.

Further, even if Hanson was properly combinable with the admitted prior and Bissell, the combination would still fail to render obvious the invention of the rejected claims. For example, in connection with claim 19, the Examiner takes the position that the templates recited by that claim are taught by Hanson. However, while Hanson does use the term "template" in his disclosure, it is in connection with providing a starting point for the creation of an action message on behalf of an end user, not for use in determining whether a control data message is proper by such templates corresponding to approved control data messages. There are similar disparities in the application of Hanson in the rejection of the remaining dependent claims including, but not limited to, claims 20 and 21 that further address templates.

Thus, for the reasons presented above, claims 1 – 24 are considered to be allowable over the art of record and withdrawal of the outstanding rejection thereof under 35 U.S.C. §103(a) is respectfully requested.

Claims 25-32 and 34-38

Claims 25-32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over applicants' admitted prior art in view of Sawyer, claim 34 further in view of Bissell and claims 35-38 further in view of Hanson et al. (6,014,427). These rejections are respectfully traversed in view of the present amendments to the claims emphasizing the time stamp aspect of the invention for determining whether control data messages are timely and properly sequenced. The rejection is further traversed as being improperly based on hindsight, the Examiner having failed to identify legally cognizable motivation for making the asserted combinations.

It is once again noted that claim 33, not having been included in the statement of the rejection in the Detailed Action, is considered to be allowable with no prior art having been applied against the subject matter recited therein.

Addressing the detailed rejection of claim 25 together with claims 26-32 and 34 – 38 dependent therefrom, the Examiner initially states that the admitted prior art discloses what

amounts to the first step of claim 25, i.e., exchanging control data message between a remote communication network and a local signaling communication system. For the remaining four steps of the claim the Examiner relies on Sawyer:

> *Sawyer discloses an authentication server on an SS7 network (Fig. 1 part 80) that is configured to exchange and maintain encryption key certificates (column 5 lines 27-33). Sawyer teaches that the system uses the X.509 protocol. The X.509 is a digital certificate that is distributed in order to authenticate the user. Sawyer discloses a digital signature; digital signatures are decrypted in order to authenticate the signature. This information is used to authenticate the terminal 10; and then therefore selectively provide the connection for the terminal.*

The Examiner considers the combination together with the admitted prior art to be proper because:

> *At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use digital certificates as in Sawyer in the system as disclosed in applicants' admitted prior art. One of ordinary skill in the art would have been motivated to do this because digital certificates assert that the specific token is linked to a unique person at a specific time and date.*

As an initial matter, it is difficult to understand why one skilled in the art of communications networks, having before them the single step of exchanging control data messages between networks, would be so motivated so as to implement the remaining four steps of claim 25. The motivation for such combination can only be found in hindsight based on applicants' disclosure. This is further evident as applicants' certificates are assigned to networks or network elements, not to persons as per the prior art such that, even if made, the combination would fail to describe or suggest the subject matter of the rejected claims including, for example:

> *decrypting a certificate portion of said control messages so as to authenticate origination point code information.*

Unlike the claimed invention, Sawyer is directed to certifying (digitally signing) a telecommunications service. According to Sawyer, an AIN (Advanced Intelligent Network) is used to collect a type of authentication code, whether a PIN or time-dependent authenticator. Some type of byte code indicating that the subscriber has been authenticated is passed across the SS7 network to another AIN (SCP) where the information is translated into a code to deliver

Caller ID that is verifiable to the receiving subscriber. In contrast, applicants' invention is directed to authenticating service information (i.e., Caller ID) and not the SS7 signaling protocol that is employed to control the PSTN switches. Further, as amended, the claims specifically require message authentication using a time stamp to determine message timeliness and sequencing. In Sawyer, the purpose is to vouchsafe a calling party's identity, not a network element connecting to the SS7 network as is applicants' invention. Not only does the prior art fail to describe or suggest such a feature, but the environment of the invention and the problem addressed thereby so significantly different from that described by the applied art for the reasons presented *supra* go to be un-combinable under the statute. These differences further render non-obvious the modification of the admitted prior art as suggested by the Examiner.

Lacking motivation supplied by the prior art for making the asserted combination, the outstanding rejection under 35 U.S.C. § 103(a) is improper and withdrawal thereof is respectfully solicited. The mere fact that one skilled in the art could have decided to include a certificate portion of a control message is insufficient where there was no motivation found in the prior art to do so. It is not sufficient for the Examiner to provide rational based on the hindsight realization of benefits provided by the combination; there must be motivation provided by the references (see discussion above in connection with the rejection of claims 1 – 24). Here, there is no such motivation provided by the prior art. See M.P.E.P. § 2143.01: *Suggestion or Motivation To Modify the References.*

Further, since Sawyer is directed to certifying a telecommunications service, the proposed modification suggested by the reference would at most suggest authentication of a subscriber. Implementation of this modification would thereby change the principle of operation of the admitted prior art by requiring specialized equipment as part of the terminal equipment. Thus, even if there were motivation for making the asserted combination, it would still be improper: if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. See *Id.*

The rejection is further rendered improper by the present amendment to claim 25 reciting a step of:

> *decrypting a certificate portion of said control messages including a time stamp so as to authenticate origination point code information based on said time stamp so as to determine control message timeliness and sequencing*

This feature prevents "replay" attacks which, in turn, prevents fraudulent communication form an illegitimate user purported to be authorized users requesting service at a different time than the original request. Again, failing to appreciate the interface problems to which the present invention is directed, it is to be expected that the applied art would be deficient in describing a solution to such unrecognized problem Failing to teach use of a time stamp to determine control message timeliness and sequencing, the applied art fails to anticipate or render obvious the subject matter of claim 25 and withdrawal of the corresponding rejection is respectfully requested.

The rejected dependent claims are further considered to be allowable as reciting additional subject matter not found in the art of record. For example, the Examiner rejects claim 34 over the admitted prior and Sawyer in view of Bissell. Again, there is simply no motivation supplied by the prior art for making this combination and, therefore, the rejection under 35 U.S.C. §103(a) is considered to be improper. Further, even if proper, the states mention by Bissell are different from the permissible states recited, e.g., claim 34 as discussed above in connection with claim 7.

In connection with claim 35 – 38, the Examiner again relies on Hanson. However, this rejection and its application of Hanson is likewise believed to be improper for the reasons described above in connection with claim 18 – 24.

For the reason presented, the rejections of claims 25 – 32 and 34 – 38 are believed improper and withdrawal thereof is respectfully requested.

Application No.: 09/767,292 Docket No.: 00-VE04.75B CIP

Conclusion

In view of the above amendment, applicants believe the pending application is in condition for allowance.

Applicants have filed concurrently herewith a Petition for a Two-Month Extension of Time. However, if any other or additional fee is due, please charge our Deposit Account No. 07-2347 from which the undersigned is authorized to draw and please credit any excess fees to such deposit account.

Joel Wall Reg. No 25,648

Verizon Corporate Services Group
600 Hidden Ridge Drive
Mail Code: HQE03H14
Irving, Texas 75038
(972) 718-4800
CUSTOMER NO. 32127
Date: February 7, 2005